HUMINT communication information systems for complex warfare

Luc PIGEON
Defence R&D Canada Valcartier,
Information and Knowledge Management Section,
Val-Bélair (Québec),
G3J 1X5, Canada;
Luc.Pigeon@drdc-rddc.gc.ca

Clark J. BEAMISH
Directorate of Army Doctrine
PO Box 17000
Station Forces
Kingston (Ontario),
K7K 7B4, Canada;
beamish.cj@forces.ca

Michel ZYBALA
National Counter Intelligence Unit
Toronto Detachment,
40 Woodhead Crescent
North York (Ontario),
M3M 2Z5, Canada.

Abstract

Human intelligence (HUMINT) is one of the most versatile and powerful information sources available for situation awareness and decision-making. Its low cost and ready availability could make it the silver bullet of intelligence. This is particularly true within urban operations and operations in complex terrain, where technically acquired information may be degraded by that particular environment. Unfortunately, there are several drawbacks to HUMINT, in that it can be time-consuming; it may take several months to initially set up effective contacts in a particular environment; and it can be susceptible to deception. This paper proposes a framework for HUMINT and counter-HUMINT communication information system (CIS) development. The proposed framework is built to include both legacy HUMINT analytical processes/systems and to define new criteria for future HUMINT operations regarding information collection and information management. Objectives and accuracy achievements are proposed through the DITE (detection, identification, track, and estimate of future state) sequence of events. Data is structured by five-dimensions based on space, time and possible worlds. Processing is proposed with respect to common ontology, data merging and data fusion, resources management and learning capabilities. Examples illustrate the CIS design for C-HUMINT, social networks, and urban operations human intelligence assessment.

1. Introduction

Human intelligence (HUMINT) is defined as *a category of intelligence derived from information collected and provided by human sources* [INSCOM, 2001]. It is a Foreign Intelligence Activity focused on the penetration of an adversary's decision making architecture to obtain information regarding capabilities, vulnerabilities, disposition, plans and intentions [INSCOM, 2001]. Its components are categorized by directed conventional activity, military intelligence liaison, and field HUMINT (military intelligence reconnaissance, screening, debriefing, interrogation, contact handling, agent handling, covert passive surveillance and specialist technical support) [JWP, 2000].

HUMINT is one of the most versatile and powerful information sources available for situation awareness and decision-making. Its low cost and ready availability could make it the silver bullet of intelligence. This is particularly true within urban operations and operations in complex terrain, where

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
SEP 2002		**00-00-2002 to 00-00-2002**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
HUMINT communication information systems for complex warfare	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defence R&D Canada Valcartier,Informaiton and Knowledge Managment Section,Val-Belair (Quebec),G3J 1X5 Canada, ,**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**15**	

technically acquired information may be degraded by that particular environment. Unfortunately, it has been traditionally overshadowed by drawbacks related to the length of time it may take to acquire the desired information and HUMINT's vulnerability to deception.

In the Cold War, imagery intelligence (IMINT) and signals intelligence (SIGINT) provided the bulk of our Intelligence on the adversary. This type of information, once analyzed, provided sufficient intelligence for decision-makers because they already knew the adversary's intent. In today's environment, these capabilities are no longer sufficient.) Strategic level IMINT and SIGINT agencies (e.g. NIMA and NSA) continue to increase their technical collection capabilities, but the gray areas concerning intent continue to exist and they continue to essentially provide a record of what is where.

In recent history, in the Air Campaign in Yugoslavia for example, Western aircraft successfully attacked a myriad of decoys. In reality, the vast majority of Yugoslav military hardware was left untouched. By the second week, when NATO perceived that it had run out of military targets, it turned to civilian and government infrastructure, with all the unfortunate collateral damage that was made immediately available for the world to see. In asymmetric warfare in complex terrain, operations will be likely characterized by non-uniformed combatants mixing in with the general population. With the potential for degraded IMINT and SIGINT, HUMINT gains a new importance and relevance to the overall information collection effort. In the case of Yugoslavia, the adversary was in uniform, but the West lacked the wherewithal to effectively satisfy its PIRs regarding the disposition of the real equipment and the actual intent for its use. Unfortunately for the West, relying upon technically acquired information, the strategic, operational and tactical levels of operations became blurred. This resulted in even more importance placed on technically acquired information. Unable to determine what decisions were being made by commanders and the morale and physical condition of soldiers and equipment, the West was unable to forecast what the enemy intended to do with its forces. In this case, the intent was to hide and camouflage everything. While HUMINT is not the only means to determine intent and provide early warning of adversary actions, it has the potential to be one of the best. HUMINT is also valuable in assessing battlefield damage and in the case of the air campaign in Yugoslavia; HUMINT could have been a valuable asset in determining the effectiveness of the campaign.

Recently, there has been a realization amongst senior leadership of the value of HUMINT in its potential to confirm IMINT and SIGINT. Furthermore, it has been now acknowledged that the true value of HUMINT is its potential to realize adversary intent and not just to confirm the existence of what has been imaged or located. This is what decision-makers will need for future operations. HUMINT also possesses the capability to make a contribution to both the offensive and defensive aspects of intelligence. While HUMINT techniques can be employed to influence friendly visualization of an adversary, the same techniques are employed by the counterintelligence (CI) specialists to influence an adversary's visualization of friendly capabilities and intent by identifying, neutralizing or exploiting hostile HUMINT assets. HUMINT's inherent flexibility allows it to be used both as a shield and as a sword.

On the down side, since HUMINT techniques involved in the offensive and defensive aspects of intelligence are the same, the sources are quite often the same. This opens up the possibility of HUMINT agencies (be they intelligence, security intelligence or law enforcement) with widely differing

organizational objectives and legal mandates competing for the same information. Moreover, HUMINT cannot be generated overnight and since it covers a wide range of activities it can be highly complex. Thinking of HUMINT as a sensor, the main difference from other sensor capabilities is that the HUMINT sensor is not material. It rather consists exclusively of human beings and human interaction. Therefore, it exists in a world of subjective deduction. The information collected is often the result of a chain of human interactions and human interpretations. It is sometimes influenced by cultural and environmental factors that may become relevant for many reasons, some of which might be real and others which may be part of an adversary deception operation.

Imagine a series of concentric circles, one within another, representing the core, extended and virtual families of HUMINT. Reaching out through the breadth and depth of an operation, the circles represent the amount of information available to the people at the center. In the outer circle, the information might represent the Internet and demographic information available in the public domain, as well as contacts, agents and available databases. The next inner circle might represent the military environment, including other sensor systems, strategic and operational level support and available databases. The innermost circle might represent the Field HUMINT Team. All the outer circles feed information inwards, the ebb and flow being dictated by inquiries from the center and by planned and unplanned external activities and events. This series of concentric circles provides a view of the information flow in the HUMINT environment.

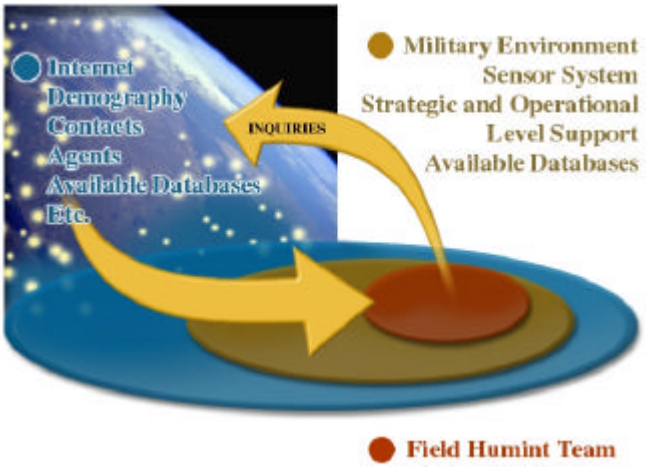

Figure 1: Information flow in the HUMINT environment

At the core, highly qualified analysts, with the right skill sets and experience can bring HUMINT to its full potential. However, this environment is complicated by the human factor, a general lack of human capacity to rapidly integrate and reference large amounts of information. Moreover, when information overload does occur in HUMINT, especially in a stressful environment, the susceptibility to deception increases. In addition, key facts may be overlooked, reducing the value of the HUMINT product itself and forcing decision-makers to place more reliance on technology, which may or may not provide them with the answers to their PIRs. This situation can be corrected somewhat by providing the HUMINT analyst with a good communication information systems (CIS) architecture that can provide him with powerful data fusion, link analysis, cross-referencing (research) and information dissemination capabilities.

It should also be noted that the development of a HUMINT capability could take decades to become effective. It requires a long-term commitment from the highest levels of command and government for that matter. It requires extensive, meticulous records spanning months if not years. For example, in the case of the UK and Sierra Leone, they have been involved in four operations in that country over the decades. The challenge of maintaining records and contacts over that span of time would be almost unthinkable in Canadian terms. And yet, with the myriad of operations in which Canada now finds itself becoming involved, the long-term maintenance of records and contacts will become a reality. The records and databases will not only have to cover specific operations over time, but also different venues of operation, such as peacekeeping, peacemaking and mid-intensity conflict in a variety of coalitions. Accurate, reliable, responsive, relational database management is one of the main challenges facing HUMINT in its duties in future operations.

In order to address the magnitude of this challenge facing the Canadian military community regarding HUMINT, this paper proposes a framework for HUMINT CIS development encompassing the HUMINT operator, the information and the information environment. The proposed framework would be built to include both legacy HUMINT analytical processes/systems and future HUMINT systems. For the latter, new criteria need to be defined regarding information collection and information processing, including management. The proposed CIS framework involves semi-automation, which is an approach whereby the human-analytical capabilities are enhanced by their machine counterparts. The proposed CIS aims to cope with an ever-expanding Military Information Environment (MIE) and Global Information Environment (GIE), and to ultimately maximize the holistic contribution of HUMINT to decision-making. Section 2 presents a proposal for the design of HUMINT CIS. It is described with regard to the interface, the data structure and the processing. Section 3 exemplifies this CIS with social networks and urban operations.

2. **HUMINT CIS Design**

This section is about a HUMINT CIS design based on the information system design suggested by [Pigeon, 2002]. The architecture is defined from three facets: interface, data structure, and processing. The interface is considered as the link between the physical-system and its users and is characterized by goal definitions, required accuracies and determination of sequence of events. The proposed data structure is based on the world physical representation of space and time. A possible-worlds dimension enhances the system to support *a priori* knowledge of the problem, simulations, as well as the recording of past events. The processing unit of the proposed system design handled data fusion and resources management and enhanced a learning component definition, which introduces "intelligence" within the system.

For the purpose of this paper, these three facets are applied to CIS definition. However, they could be applied at many levels of abstraction, ranging from the CIS design to the operations execution modeling. This logical framework could then be applied to characterize concepts nested within other concepts. To avoid confusion, special attention should be paid to this observation.

2.1 ***Interface***

This subsection presents the link between the physical-system and its users with regard to identification of objectives, of accuracies, and of sequence of events.

2.2.1 ***Objectives***

From the HUMINT definition, HUMINT CIS inputs are *information collected and provided by human sources*. From [INSCOM, 2001] the aimed output is information regarding capabilities, vulnerabilities, disposition, plans and intentions. The primary value of HUMINT is its potential to realize adversary intent. The secondary value is its capability to enhance SIGINT and IMINT to confirm the existence of what has been imaged or located. Hence intelligence covers both questions about *what is where*, and *why and what for*. As mentioned earlier, the value of HUMINT, or more specifically of counter-HUMINT (C-HUMINT), can also be found in its ability to influence how an adversary perceives our own capabilities, vulnerabilities, dispositions, plans and intentions. Having used C-HUMINT techniques to identify a hostile HUMINT asset, a move can be performed to either neutralize this asset (e.g. executing an arrest) or to exploit it (either by "turning" an arrested enemy agent into a double agent, or by feeding him a deception). In any event, C-HUMINT can be used to create uncertainty in the mind of an adversary by degrading his capability to conduct HUMINT collection. While the work of a HUMINT analyst is completed, a C-HUMINT specialist is often required to make a transition from passive reporting to active countermeasures (e.g. investigation, raid, and arrest). In order to achieve the objectives, a robust CIS design should increase actual HUMINT strengths, while reducing its weaknesses. Based on [Army Lesson Learned Centre, 2001][JWP, 2000] and [Betts, 2002], table 1 lists HUMINT advantages and disadvantages.

Advantages	**Disadvantages**
Almost permanent availability i.e. all time (24hours/day, 7days/week) and all-weather collection availability.	Collected data is unstructured, then difficult to process and exploit.
	Information expiration can occur from the lag between collection, processing and dissemination.
	Target areas data transmission and fusion are often inadequate and difficult to perform.
Low dependence on technical support for collection and processing.	Required robust command, control and communication system (C3IS) for enhanced processing, communications and coordination. Appropriate protection must always be afforded for HUMINT collection operations.
Versatility for re-tasking.	Dependence on C3IS robustness for coordination.
Intelligent sensors (human being) characterized by initiative and analysis capabilities.	Subject to deception and enemy information operations.
	Source reliability and information credibility are often difficult to assess.
Training, preparation and running cost relatively low compared with other collection systems.	Contact and agent handling are long to initiate.
	Culture knowledge, particularly language, represents a HUMINT limitation that is difficult to assess for future operations (collection and processing).

Table 1: HUMINT advantages and disadvantages.

A marked HUMINT advantage is the capability to accommodate both the offensive and the defensive aspects of military intelligence, as well as the needs of law enforcement. The disadvantage is that while the techniques are similar, so are the sources, opening up the possibility for conflict between agencies that use similar information and sources for different purposes.

Democratic societies generally make a clear distinction between their security and intelligence apparatus, on the one side, and their law enforcement apparatus, on the other (functional distinctions reinforced by legal barriers). The problem in our modern world is that the "Bad Guys" do not feel obligated to comply with these distinctions. Many terrorist organizations will routinely turn to crime to finance their activities. Criminal organizations will sometimes employ terrorist tactics in the interest of protecting their criminal enterprises (i.e. the Mafia bombing the Ufizzi Art Gallery in Florence). In Bosnia, intelligence services entities were seen involving themselves in crime as a profitable sideline.

As an example, Terrorist Group A is planning an operation against a US military facility. Their plan is to gain access to the facility by disguising themselves as Canadian servicemen. In furtherance of their plan, they break into a military base's clothing store and steal some uniforms. Theoretically, from an IS perspective, the information have to be managed both as a security intelligence problem (i.e. with a view to thwarting a planned terror attack), and as a law enforcement problem (with a view to successfully prosecuting the offenders in front of a very public and duly constituted tribunal. Practically, answers have to be found about the reconciliation of the competing information management requirements so that they do not come into conflict, but complement each other.

HUMINT disadvantages might be assessed through the next objectives. At the system level, an effective design should reduce significantly the lag within the intelligence cycle: direction, collection, processing and dissemination [Canada National Defence, 1998]. Data transmissions can be constrained and enhanced by CIS objectives/accuracy/sequence, structure and processing. The protection of HUMINT operations is related to system integrity, including humans as components. Architecture should then be characterized by robust design and protected by strict doctrinal use, software security and strong CI monitoring.

At the data structure level, disadvantages related to unstructured data could be minimized by a formal structure (2.2). From this perspective, cultural knowledge could be formalized and be ready for processing. At the processing level, data-fusion can be performed and enhanced with structured inputs and formal processing methods. Results should improve analyst capabilities to detect deception and adversary operations. Source reliability and information credibility could be assessed through the system's learning component.

Objectives must the defined similarly to the strategic/operational/tactic level of abstraction. For instance, the objective of CIS transmissions might state that HUMINT success is absolutely governed by the efficient passage of information. Data sharing involves communication within the HUMINT cell, with allies, and with higher headquarters. As well, inter-operability with national military and allied HUMINT organizations is fundamental to effective HUMINT operations. An objective could state that software

security by communications between the system and its components, or any open-source, must be secured against possible malicious intrusion or extraction of information. At another level of abstraction, software technical specifications could be provided. For instance, a statement could posit that a restricted number of administrators control the integrity of the storage unit structure and that multi-users access be essentially "read-only". At another level of abstraction, names of administration and users could be listed, etc.

The same thing applies to the system architecture. Strategic objectives (for CIS design) could provide the capability to realize adversary intent and be complementary to SIGINT and IMINT. At another level of abstraction, objectives could be to:

- Handle high amounts of raw data;
- quickly research complex networks to obtain key information;
- readily integrate new components and other systems i.e. upgradeable without major architectural change;
- include learning components for parameter optimization;
- aim for real time performance for transmission;
- include semi-automatic components to assist the HUMINT members in their functional tasks which might include the automated correlation of relational activities and the automated aggregation of events by time, location, structure, activity, *modus operandi*, characteristics and demography;
- include information storage, information display and communication;
- include information processing such as data and information fusion components; and
- arbitrate the competing/complementary interests of various military/civilian agencies requiring access to the same HUMINT information for different goals.

Finally, at another level of abstraction the objectives involve providing distributed storage units, distributed collection devices, distributed HUMINT analysis stations, distributed command and control systems, etc.

2.2.2. ***Required accuracy***

For each objective, the associated accuracy is based on the quantification of the previous requirements. It does correspond to the error or tolerance associated to the previous objectives. For example, a time lag acceptable requirement could differ from one task to another. Consequently, tasks should be identified and their links for transmission qualified by a time t for context c. Robustness for CIS design has also to be defined. It is directly related to system components inputs and output accuracies, and certainties [Pigeon, 2002]. If the learning component can assess these quantities, their accepted accuracies or associated confidence remain to be defined within the accuracy system part. Security requirement for software might be quantified by a list of parameters. Finally, for the human system's components, CI monitoring must ensure integrity with respect to quantified guidelines.

2.2.3. ***Sequence of events***

The next steps are a generic sequence proposal for objectives achievement. These steps are sequential: they detect, identify, track and estimate future state (DITE). They are fulfilled with regard to the context of the problem to solve.

- **Detect**: discover or perceive the existence of an object.
- **Identify**: quantify object attributes in order to meet conditions for perfect exhaustiveness and/or precision (section 4.4.1).
- **Track**: monitor the object with regard to the time dimension (section 3.2).
- **Estimate future state**: predict an object (including situation) status over time, or more particularly a damage estimate for a possible engagement, as stated by [Steinberg, 2001] level 3.

This sequence is a discrete representation of a continuum. For instance, the *identify* step can be defined as a composite of the two sub-steps that aim identification of the

1. object **category**: exclusivity (section 4.4.1) condition is not met i.e. exclusivity is considered being imperfect with regard to the context of the problem.
2. object **instance**: exclusivity condition is met i.e. exclusivity is considered being perfect with regard to the context of the problem.

This sequence can be applied to different levels of the problem. In the context of CIS design, this sequence is constrained by the system storage (section 2.3) and by the processing (section 2.4) parameters. For example, from the C-HUMINT perspective, the theft of military uniforms by a terrorist group constitutes an intelligence indicator of a potential terrorist attack. Using the DITE acronym, the first step is to **detect (D)** the occurrence as being of CI interest. However, to a military police Corporal attending the scene, the incident is nothing more than a B&E and would be treated purely as a law enforcement matter. All information regarding the incident would be entered on military police information systems, with no thought to the possibility that this B&E could have military CI implications. From the outset, we have the makings of an intelligence failure resulting from two CF organizations failing to communicate.

On the other hand, a C-HUMINT CIS that possesses the capability to tie into the MP system and to share information might apprise the CI analyst of any instances involving military police investigating a theft of uniforms. As the MP corporal finishes entering the incident into a Daily Occurrence Book (DOB) entry on the MP system, the C-HUMINT CIS might pick up on it. Having detected the incident, the CIS could use *a priori* knowledge to **identify (I)** this incident as being of CI interest. For instance, the system can highlight the fact that, during the break in, the thieves stole only uniforms, but failed to break in to the clothing stores cash register and take any money. As a further example, the military police attending the crime scene might have lifted fingerprints of a petty criminal with family ties to Terrorist Group A.

At this point, the challenge is more at the organizational level than at the scientific level. Solutions have to be found to access this kind of information for the purposes of CI without causing prejudice to the military police criminal investigation or a subsequent prosecution in court. Military HUMINT, counter-HUMINT, and criminal intelligence, are all subdivisions of a single whole intelligence. Unfortunately, the intelligence community often looses of sight the fact that this information is all interrelated and that organizational considerations create all kinds of barriers, which precludes the sharing of this information.

Answers have to be proposed in order to structure CIS system to share information, while at the same time it respects legitimate restrictions (such as those based in the law, required for the safeguard of various legal rights).

2.2 *CIS Data structure*

The structure of data-storage has to be both generic, to allow system evolution, and formal, to facilitate data processing. The proposed structure is based on the world physical representation of space and time. The dimensions space, time and possible worlds are defined below according to [Pigeon, 2002].

2.2.1 *Space*

Using the space representation (x,y,z coordinates) as data-storage structure for an object offers the advantage of being both generic and formal. Whether a single infantryman or an order of battle (ORBAT) can be modeled within these space coordinates. For both, space coordinates could characterize the instances of class. Moreover, the relationships between the ORBAT objects (situation level) and the spatial coordinates of each component can be obtained from an abstraction zoom on the desired object. Non-spatial information can be stored within the object's attributes section (example: cultural knowledge related to individuals, people networks, situations). Spatial and non-spatial accuracy should characterize object attributes. Finally, the object physical constraints can be stored within the object operations section. For example, a fuzzy value such as the enemy "will to fight", could be stored within an enemy ORBAT instance attributes section. It could even be stored on sub-parts of the ORBAT if it applied only to a subset of units. In the same way, terrain navigation constraints for a particular tank model could be stored within the object class allowed operations section, and so on.

2.2.2. *Time*

The dimension of time has to be formalized in order to handle the evolution of spatial objects (including situations) over time. Also, the time dimension might be used to store knowledge related to a resource capability available over time. Proposal is to consider the time being handled as an object attribute. From this dimension, primitive estimate of future state could be assessed. However, prediction involves the exploration of all system parameters and possibilities for single or multiple contexts. Another dimension is proposed to handle these "possible worlds".

2.2.3. *Possible-worlds*

The possible-worlds concept is the result of a dimension (w) added to the previous space (x,y,z) and time (t) dimensions. Hence, situation possible COA could be stored within a (x,y,z,t,w) format. Moreover, the predictions (estimation of future states) and the prior knowledge related to COA could be generated within this format. Historically, system component parameters from experiences -used cases- could be managed with this dimension, which is the main data source for system learning and process refinements. The ensemble of stored data constitutes the system's intellectual patrimony. Data collection involves object and time structure. Processing and analysis weigh collected objects (including

time-attribute), and generate the possible-worlds dimension. From this data structure, powerful data fusion, link and cross-referencing analysis, and selection of appropriate recipients for information dissemination could be undertaken.

2.3 *CIS Processing capabilities*

Data exploitation can be achieved with respect to a common ontology and to appropriate analysis tools that enhance analyst capabilities to highlight key information and quickly unravel complex networks. This can be achieved through information merging, more evolved data fusion, and system learning components.

2.3.1 *Ontology*

Common ontology extended the concept of data alignment [Steinberg, 2001] to include inter-agency shared data as well as legacy data, within the proposed data structure proposed in section 2.2.2. A system component (subsystem) should then be assigned to perform this linkage. For legacy integration, the sub-objectives of the system could involve the storing of the last decades reports (being previously digitalized), their translation into a single language, the recognition of handwritten characters, the recognition of key words and patterns, and the information processing to achieve linkage to the object/time/possible-worlds (x,y,z,t,w) format.

To facilitate data integration, new reports should follow a logical easily filled out format. The means can be electronic -if the equipment is available- or handwritten. In the latter case, a structured format should be used with respect to a system docking facility. This should include a place for free text and must be written with the purpose of capturing key data. A preset formatted paper form should facilitate this process. Data alignment also concerns weight assignment to incoming data in order to process information with respect to source reliability and information credibility. Weight assignment should be extended to the ensemble of system's data, especially to component decisions.

2.3.2 *Analysis*

Information merging corresponds to an access to the all-data storage. Since CIS involves distributed data storage, a secure transparent process must assess relevant data access, transmission and visualization. Relevant data being chosen by the command or determined by the system from identify, track and estimate future state (ITE) sequences. Hence, from the system capability to estimate a situation future state, possible worlds could be generated (w dimension) and a restraint all-data subset become relevant for access, transmission and visualization.

From the a priori knowledge of problems, inference networks can be generated. These networks are nothing but conceptual maps, showing possible paths to take in order to navigate from one point to another. These logical paths relate data to objectives, with checkpoints that could merge data and decisions. They are firstly defined from a prior knowledge about problem solving. Subsequently, they can be enhanced by a learning component. Then, from structured data, particularly inference networks,

a component can assess complex networks unraveling to highlight key information. However, when inference redundancy occurs, data fusion has to be performed. A possible definition for data fusion [Li *et al.*, 1993] may be generalized to "the combination of a group of inputs with the objective of producing a single output of greater quality and reliability".

The purpose of fusion is to reduce the redundancy of links (information overload) and/or to improve accuracy by summing partial data or uncertain data. Reversing this process could lead to the identification of the place where the redundancy of links is required and/or of the context to use complementary sources for problem solving. Consequently, fusion achieves combination of links in order to rank solution hypotheses. The decision process remains as a separate step performed by command. Fusion can also be achieved at the model level [Pigeon, 2002]. The fusion of these models, which can also be modeled within the (x,y,z,t,w) structure, is defined by the process of combining inference links together in order to produce a single inference link of improved quality. For example, these links could be mathematical models [Pigeon *et al.*, 2001] that, taken separately do not allow inference from a data source to a solution, but taken together can bring the system to a single solution (or to another inference, since fusion can occur at many levels). Model fusion can also be applied to mixed data fusion i.e. to pieces of data characterized by different imperfections.

A resource management subsystem design is proposed [Pigeon, 2002]. Management could be applied to a single resource and/or to a network of resources to handle their collection. From possible-worlds knowledge and learning capacities, the system should be able to predict the impact of resource on the system state i.e. system time-response to requests, bandwidth bottlenecks, tasks, etc. Constructive or destructive interferences have to be assessed in the same phase. From cost functions, optimal path e.g. possible course of actions (COAs), within space and time dimensions, could be generated (synchronously or asynchronously) for resources management. To complete the processing facet, a CIS learning capability could assess and optimize the system's components performance [Pigeon, 2002].

3. **Complex warfare application – Urban operations**

The next examples apply the HUMINT CIS proposed design within situations. Each example illustrates the CIS objectives and accuracy, and the sequence DITE with respect to the proposed data-structure and to the proposed processing tools. The first example assesses HUMINT for social network information gathering. The second example presents a CIS application within urban operations.

3.1 ***Social network example***

The objectives of the example are: a - identify (I) key people in the area of operations; b- identify (I) links between key people (occurrence of a relationship between objects, which can binary, 0 or 1, or fuzzy, 0 to 1); c- estimate operations on the critical points of the network of people. The accuracy of the objectives is: a- definition of "key people" i.e. leaders in the fields of politic, economy, religion, civil affairs, families; b- definition of search areas i.e. the borders (e.g. country, province, and district). In order to get identification (I), previous sequential steps have to be completed. Then for identification, detect and recognize are the first steps to be undertaken. To identify key persons, these have first to be

detected (D). This could be performed by inter-agency data sharing, searching the Internet, by social patrolling, or every other means that bring a person's occurrence (name, picture, reference, etc.) within our system. From this point, based on the proposed data structure, the information gathering process aims to fill the object's name, its attributes, and its permitted operations (i.e. possible influential relationships with other objects). Links with other objects could also be assessed at this moment.

(a) **(b)**

Figure 2: Category (a) and instance (b) identification – social network assessment

Figure 2 shows examples of objects at the recognition level. In figure 2a, two men are categorized but their identification remains imprecise. The instance of the woman is already identified. This situation describes a man (possibly a criminal) calling a woman (Natalia). After the phone call, Natalia transfers 50000$ to the bank account holder, a man linked with the national military organization. With information collection, the two instances of men are identified (figure 1b). Barbarcaf, is a member of the local mafia, which provides armament to a terrorist group. Paul, a sergeant of the infantry, is the uncle of Natalia. From this point, link analysis can be performed to learn about a possible link between Barbarcaf and Paul, maybe revealing information about the provenance of the terrorist group weapons. More generally, a series of events/situations are tracked, confirming or denying existing linkages and other events/situations. At a certain point deductions are produced regarding the linkages, which of course lead to other linkages and finally to simulation or modeling.

A breakout function has to be defined to validate the pursuing or the interruption of the process. A suspect could reveal itself of no interest at a certain point, then it could be decided that no more efforts might be assigned to its case. Normally, the human analyst is aware of this threshold. The passage from recognition to identification is set from the exclusivity condition. The exclusive condition means that the object is unique and that the occurrence of all its parameters concerns only that object. In the area of databases, the key field requirement concerns the exclusive condition. For instance, an individual name is not enough to characterize somebody as unique i.e. without confusion. With regard to the context, the national identity number could be enough to meet exclusiveness. In some other context, digital prints could be added, etc. Person identification can rely on particular characteristics or behaviors. From

them, a link with the person's object representation is accessible if a prior knowledge of this person identification exists. For link definition instead of object definition, exclusivity becomes precision [Pigeon, 2002]. An aggregation of object forms a group. Each individual is member of one group and certainly also of many groups. Figure 3a illustrates the overlapping between individual memberships to social groups. Paul and Natalia are members of the *family* group. Natalia can also be a member, with Barbarcaf, of the group *criminal organization*. Barbarcaf, is also a member of the group *mafia*, etc. Figure 3b presents the possible interactions between instances of social groups such as government, military, civil, religion, police, and family.

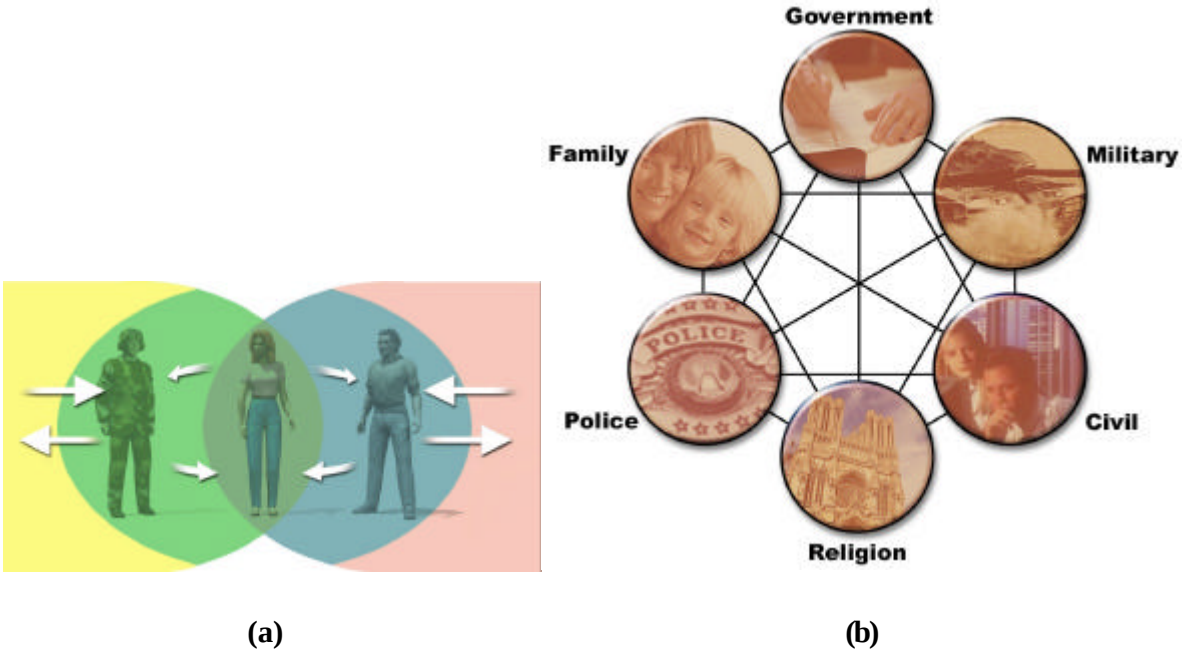

Figure 3: Social network assessment: a) Person representation level; and (b) Situation representation level.

An events diagram can illustrate the object variability over time. For a particular situation, a social structure for instance, events of interest could have been recorded. From a permanent update of the situation (the tracking sequence of DITE) a clear view of the evolution of a situation becomes available (x,y,z,t). From this knowledge, estimation of future state could be achieved. Simulations might be performed to estimate possible worlds (w dimension) with regard to targeted parameters variations. At this level, parameters can be set in order to estimate the impact of an intervention on particular network nodes. Moreover, the reverse process could be executed to identify (I sequence) network nodes that are critical points in order to achieve a desired result.

3.2 *Urban operations example*

Another complex case is urban operations. [U.S. Army, 2000] intelligence requirements checklists for urban operations identified two categories of intelligence: culture, and city infrastructure and services. The social network example is involved in the cultural category. This example could be enhanced by

details related to the type of identification that are required or in use in the urban area. They can be listed by national, local, government service, military, driver's license, professional/trade/union, voters, photo Ids, etc. Previous information could link to the person or to the organization that issued the document, or to the requirements for obtaining it, or to the location where it was issued, etc. For a crisis management representation, a city object might be characterized by attributes related to decision makers, civil alert system (if it does exist), civil evacuation plan, alert communication system, etc. The alert communication system could be characterized by attributes of effectiveness, test frequency, etc. In summary, at the CIS level, the object selection is achieved from the mission objectives and their related accuracy. The DITE sequence is then applied by the processing tools, with respect to the data structure (x,y,z,t,w). Then the intelligence cycle is performed as a loop until the command decides that the breakdown condition is fulfilled.

4. Conclusion

[Betts, 2002] points out that it is better to invest in competent people to analyze collected information than in spies. However, these analysts are only competent if they have the right skill sets and have the proper support. Pumping up the rank of analyst can make a difference within the relatively short time span. In the long term regarding HUMINT, a robust CIS structure must be defined. Its generation, including the human analyst as part of its components (team-mates), should aim at the acceleration and the improvement of the Intelligence cycle of direction, collection, processing, and dissemination in support of HUMINT functionality, and, it should also be comprehensive, to cut across inter-agency lines. This paper presented a possible approach for HUMINT CIS design. Its framework is based on system objectives and related accuracy requirements, constrained by a determined sequence of events, in this case detect, identify, track and estimate of a future state (DITE). A five-dimension structure is proposed for data modeling and management: space (x,y,z), time (t) and possible worlds (w). On this foundation, data exploitation and resource management can be performed with regard to common ontology and analysis. This includes network inference, data merging and data fusion capabilities. The learning process can enhance the system by an intelligent component performing optimization.

For R&D, the challenge concerns the implementation of this CIS framework, with respect to knowledge engineering, real-time constraints, information visualization, data-sharing, distributed environments, security, and finally to the most important, the people that will use it. In terms of inter-agency HUMINT challenges, the problem goes much further than information sharing between government or military security/intelligence and law enforcement agencies. The integration of the resulting information to security establishments of private sector companies and multinationals should be assessed (e.g. Canadian banks or multinationals such as General Motors). As HUMINT types, these intelligence establishments cannot be ignored, particularly given the transnational nature of terrorism and its growing symbiotic relationship with organized crime.

5. Acknowledgements

The authors would like to thank Dr. Sonia El Euch and Mr. Jean-Pierre Lapointe for their invaluable help in the production of this document. Moreover, the authors would like to thank Brigadier-General Glenn Nordick for discussions about strategic concepts, which enriched the redaction of this document.

6. References

[Army Lesson Learned Centre, 2001] *HUMINT au cours d'opérations de soutien de la paix*. Army Lesson Learned Centre, PO Box 17000 Stn Forces, Kingston, Ontario, Canada, K7K 7B4, 2001, 31 pages.

[Betts, 2002] Richard K. Betts. Fixing Intelligence. Foreign Affairs, January-February 2002, Vol.81, No. 1, pp. 43-59, 2002.

[Canada National Defence, 1998], *Land Force Information Operations: Intelligence*, Chief of the Defence Staff Publication B-GL-352-002/FT-001, 1998.

[Dick, 2001] C. J. Dick. *Conflict in a Changing World*. Part of NATO SAS-30 Urban Seminar Wargame, November 2001,12 pages.

[INSCOM, 2001] *2X Staff Handbook*. INSCOM Training and Support Detachment in coordination with USAIC&FH Counterintelligence and Human Intelligence Subject Matter Experts, May 2001, 67 pages.

[Li *et al.*, 1993] H. Li, B S. Manjunath, S.K. Mitra. *Multisensor Image Fusion using the Wavelet Transform*. Graphical Models and Image Processing, Vol. 57, pp. 235-245, 1993.

[Pigeon *et al.*, 2001] Luc Pigeon, Laurent Lecornu, Bassel Solaiman, Gnewael Brunet. *Model fusion for road extractions from multi-source satellite images*. Proceeding of. SPIE, Sensor Fusion: Architectures, Algorithms, and Applications V, Orlando, Florida, Vol. 4385, p. 140-148, April 2001.

[Pigeon, 2002] Luc Pigeon. *A Conceptual approach for military data fusion*. Submitted for the 7th International Command and Control Research and Technology Symposium, Quebec City, September 2002.

[Solaiman, 2001] Bassel Solaiman. *Information Dusion Concepts. From Information Elements Definition to the Application of Fusion Approaches*. Proc. SPIE Vol. 4385, p. 205-212, Sensor Fusion: Architectures, Algorithms, and Applications V, Orlando, Florida, April 2001.

[Steinberg, 2001] Alan N. Steinberg. *Data Fusion System Engineering*. IEEE AESS Systems Magazine, June 2001.

[JWP, 2000] United Kingdom Joint Doctrine for Defence HUMINT Activity. Joint Warfare Publication 2-01, June 2000.

[U.S. Army, 2000] Headquarters Department of the Army. *U.S. Handbook for Joint Urban Operations (2000 - Primer for future JP 3-06: Doctrine for Joint Urban Operations)*. http://www.dtic.mil/doctrine/jel/other_pubs/juohdbk1.pdf, 2000.